Advisory Action Before the Filing of an Appeal Brief	**Application No.** 10/537,300	**Applicant(s)** JOYE, MARC	
	Examiner LONGBIT CHAI	**Art Unit** 2431	

--The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

THE REPLY FILED 02 December 2008 FAILS TO PLACE THIS APPLICATION IN CONDITION FOR ALLOWANCE.

1. ☒ The reply was filed after a final rejection, but prior to or on the same day as filing a Notice of Appeal. To avoid abandonment of this application, applicant must timely file one of the following replies: (1) an amendment, affidavit, or other evidence, which places the application in condition for allowance; (2) a Notice of Appeal (with appeal fee) in compliance with 37 CFR 41.31; or (3) a Request for Continued Examination (RCE) in compliance with 37 CFR 1.114. The reply must be filed within one of the following time periods:
   a) ☒ The period for reply expires *3* months from the mailing date of the final rejection.
   b) ☐ The period for reply expires on: (1) the mailing date of this Advisory Action, or (2) the date set forth in the final rejection, whichever is later. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of the final rejection.

   Examiner Note: If box 1 is checked, check either box (a) or (b). ONLY CHECK BOX (b) WHEN THE FIRST REPLY WAS FILED WITHIN TWO MONTHS OF THE FINAL REJECTION. See MPEP 706.07(f).

Extensions of time may be obtained under 37 CFR 1.136(a). The date on which the petition under 37 CFR 1.136(a) and the appropriate extension fee have been filed is the date for purposes of determining the period of extension and the corresponding amount of the fee. The appropriate extension fee under 37 CFR 1.17(a) is calculated from: (1) the expiration date of the shortened statutory period for reply originally set in the final Office action; or (2) as set forth in (b) above, if checked. Any reply received by the Office later than three months after the mailing date of the final rejection, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

NOTICE OF APPEAL

2. ☐ The Notice of Appeal was filed on _____. A brief in compliance with 37 CFR 41.37 must be filed within two months of the date of filing the Notice of Appeal (37 CFR 41.37(a)), or any extension thereof (37 CFR 41.37(e)), to avoid dismissal of the appeal. Since a Notice of Appeal has been filed, any reply must be filed within the time period set forth in 37 CFR 41.37(a).

AMENDMENTS

3. ☐ The proposed amendment(s) filed after a final rejection, but prior to the date of filing a brief, will not be entered because
   (a) ☐ They raise new issues that would require further consideration and/or search (see NOTE below);
   (b) ☐ They raise the issue of new matter (see NOTE below);
   (c) ☐ They are not deemed to place the application in better form for appeal by materially reducing or simplifying the issues for appeal; and/or
   (d) ☐ They present additional claims without canceling a corresponding number of finally rejected claims.

   NOTE: _____. (See 37 CFR 1.116 and 41.33(a)).
4. ☐ The amendments are not in compliance with 37 CFR 1.121. See attached Notice of Non-Compliant Amendment (PTOL-324).
5. ☐ Applicant's reply has overcome the following rejection(s): _____.
6. ☐ Newly proposed or amended claim(s) _____ would be allowable if submitted in a separate, timely filed amendment canceling the non-allowable claim(s).
7. ☒ For purposes of appeal, the proposed amendment(s): a) ☐ will not be entered, or b) ☒ will be entered and an explanation of how the new or amended claims would be rejected is provided below or appended.
   The status of the claim(s) is (or will be) as follows:
   Claim(s) allowed: _____.
   Claim(s) objected to: _____.
   Claim(s) rejected: *1-8*.
   Claim(s) withdrawn from consideration: _____.

AFFIDAVIT OR OTHER EVIDENCE

8. ☐ The affidavit or other evidence filed after a final action, but before or on the date of filing a Notice of Appeal will not be entered because applicant failed to provide a showing of good and sufficient reasons why the affidavit or other evidence is necessary and was not earlier presented. See 37 CFR 1.116(e).
9. ☐ The affidavit or other evidence filed after the date of filing a Notice of Appeal, but prior to the date of filing a brief, will not be entered because the affidavit or other evidence failed to overcome all rejections under appeal and/or appellant fails to provide a showing a good and sufficient reasons why it is necessary and was not earlier presented. See 37 CFR 41.33(d)(1).
10. ☐ The affidavit or other evidence is entered. An explanation of the status of the claims after entry is below or attached.

REQUEST FOR RECONSIDERATION/OTHER

11. ☒ The request for reconsideration has been considered but does NOT place the application in condition for allowance because: See Continuation Sheet.
12. ☐ Note the attached Information *Disclosure Statement*(s). (PTO/SB/08) Paper No(s). _____
13. ☐ Other: _____.

/Longbit Chai/
Primary Examiner, Art Unit 2431

Continuation of 11. does NOT place the application in condition for allowance because:

1. Applicant asserts that Drexler fails to teach "a cryptographic method during which an integer division of the type q = a div b and/or a modular reduction of the type r = a mod b is performed, where q is a quotient, a is a number containing m bits, b is a number containing n bits, with n less than or equal to m and bn-1 is non-zero, bn-1 being the most significant bit of the number b" (Remarks: Page 3 / last Para). Examiner respectfully disagrees because (a) the claim language " q = a div b and/or a modular reduction" is considered by Examiner as merely a singular selection of "a modular reduction" as set forth in this prior-art rejection (Drexler: Para [0004], Para [0007] and Para [0020]: a modular reduction used for a encryption / decryption process), which is sufficient to meet the claim language of "and / or", (b) Y = Md mod n, as taught by Drexler (Para [0007]), is qualified as a modular reduction with Y as the result of modular reduction matching the claim language of (a type r); besides, n (as a modulus) is indeed less than or equal to Md which provides the calculation process of encryption or data scrambling (Drexler: Para [0004], Para [0012] and Para [0020]) that is also qualified as a cryptographic method, as recited in the claim, and is performed in a semiconductor chip (Drexler: Para [0011]) which contains and manipulates the data in a unit of bits in the semiconductor chip having at least one data with a nonzero MSB-bit).
2. Applicant further asserts that Drexler fails to teach "masking the number a by a random number ρ before performing the integer division and/or the modular reduction" (Remarks: Page 5 / 5th Para). Examiner respectfully disagrees because Drexler teaches a random number r is first chosen for modular process (M mod n) by forming a product of (r * n) which is added to the message M, where n is the modulus, as taught by Drexler - this is also consistent with the disclosure of the specification of the instant application (SPEC: Page 10 Line 5: i.e., for modular process (a mod b) in order to mask the number a, b times the random number ρ is added to the number a, i.e. a is replaced with a + (b * ρ)).
3. Furthermore, Applicant asserts that Drexler fails to teach "generating encrypted or decrypted data in accordance with the results of the division and/or modular reduction" (Remarks: Page 5 / 3rd Para). Examiner respectfully disagrees because Drexler teaches an encryption process with a result using (mod n) modular reduction after completion of exponential process (Drexler: Para [0020] Line 1 -3 / Line 14 - 16 and Para [0005]). Thereby Drexler does teach "generating encrypted or decrypted data in accordance with the results of the division and/or modular reduction" and as such Applicant's arguments are respectfully traversed..